Procedures Governing Use of JPAS by Cleared Contractors

Defense Security Service
April 2007

National Industrial Security Program Operating Manual (NISPOM) paragraph 2-200b states that "When the CSA [Cognizant Security Agency] has designated a database as the system of record for contractor eligibility and access, the contractor shall be responsible for annotating and maintaining the accuracy of their employees' access records. Specific procedures will be provided by the CSA." The Department of Defense, acting as a CSA, has designated the Joint Personnel Adjudication System (JPAS) as the DoD system of record for contractor eligibility and access.

JPAS is a U.S. Government information system that contains official government records. The information in JPAS must be protected from unauthorized disclosure and used only for authorized purposes. Contractors may only use their JPAS accounts to manage the access records of their employees and consultants, and to verify the access levels and affiliations (e.g., employee of ABC Company) of incoming visitors who require access to classified information.

The following procedures are issued under the authority provided by NISPOM paragraph 2-200b. Contractors shall follow these procedures when using JPAS and shall ensure that authorized users of JPAS have been properly informed about these procedures and any other specific policies governing access to and use of JPAS.

1. Contractors shall accurately maintain the JPAS records pertaining to their employees and consultants. Contractors must expeditiously update these records when changes occur (e.g., termination of employment).
2. Contractors are prohibited from placing false information in JPAS, and DSS will seek appropriate sanctions against contractors and contractor employees who knowingly place false information in JPAS.
3. DoD issues JPAS accounts exclusively for use by a specific contractor or corporate family of contractors. Persons given access to JPAS as account holders may only use JPAS on behalf of the cleared contractor or corporate family of contractors through which the account was issued. For example, an employee of ABC Company holding a JPAS account issued through ABC Company and who works at a government site is not authorized to use the contractor-granted account in support of the government customer. If the government customer requires the contractor employee to review or update JPAS records on behalf of the government customer, the government customer must provide the JPAS account for the contractor employee to use.
4. The JPAS account manager must be a company employee. The JPAS account manager cannot be a subcontractor or consultant.
5. Contractors may subcontract or obtain consultant support for administering security services. The using contractor will provide a JPAS account to the subcontractor or consultant under the using contractor's Security Management

Office (SMO) for the sole purpose of permitting the subcontractor or consultant to provide security services for the using company. Subcontractors or consultants providing such security services must be under the direct supervision of the using contractor's FSO or FSO's designee.

6. Each individual accessing JPAS must have a separate and unique account created by the individual's JPAS account manager. The account manager must maintain a current record of every JPAS account established.
7. JPAS users may never share their user names, passwords, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder.
8. Contractors must not allow any practices that include sharing user names, passwords, or other authentication information, and must have policies in place that guard against such practices. Contractors can establish JPAS accounts for additional users when a reasonable need exists.
9. Access to JPAS is only authorized by means of company or government-owned equipment with appropriate security controls in place. JPAS users may not access their accounts from personal or home computers.
10. Contractors are not permitted to change an existing date notation in JPAS for the Classified Information Nondisclosure Agreement (SF 312). Contractors must, however, input the date that the SF 312 was signed when JPAS does not reflect a date.
11. Contractors are authorized to verify prospective employees' eligibility for access to classified information in JPAS prior to an offer of employment being extended. However, contractors may not use JPAS for recruiting purposes.
12. While access to JPAS is only granted to contractors who have a legitimate need for such access in support of classified work being performed for the Government, JPAS is not a classified system. DSS will not grant a facility security clearance (FCL) for the sole purpose of allowing a company or its employees to gain access to JPAS.
13. Any contractor with JPAS access that becomes aware of a violation of these procedures shall immediately report the nature of the violation, the names of the responsible parties, and a description of remedial action taken, to the servicing DSS Industrial Security Representative.

NOTE: Violations of the procedures may lead DSS to suspend or withdraw JPAS access, terminate the JPAS account, or exclude culpable companies or persons from access to JPAS for a specified or indefinite period. DSS will also refer information concerning violations of these procedures to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.